UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/064,275	06/27/2002	Philip Lee Childs	RPS920020105	2694

53493	7590	01/09/2006	

LENOVO (US) IP Law
Mail Stop ZHHA/B675/PO Box 12195
3039 Cornwallis Road
RTP, NC 27709-2195

EXAMINER
PATEL, NIRAV B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/064,275	CHILDS ET AL.
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>27 June 2002</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-18</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>1-18</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>27 June 2002</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>9/12/02</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 6/27/02.

2. Claims 1-18 are under examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 4, 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Tait (US Pub. No. 2002/0133723) and in view of Misra et al (US Paten No.

5,757,920).

As per claim 1, Tait teaches:

submitting a user authentication request to said authentication server **[paragraph 0021**

lines 6-10, paragraph 0022 lines 1-3 Fig. 1 (receiving a message form the client at an

authorization module)**]**;

in response to a successful user authentication **[paragraph 0024 lines 1-3 Fig. 1**

(checking the credentials of the client and if valid)**]**;

receiving an authenticated user credential (i.e. ticket) which is unique to said user

[paragraph 0026 lines 10-16 Fig. 1(issuing a ticket to the client)**]**;

using said authenticated credential (i.e. ticket) to access said at least one secure resource **[paragraph 0027 lines 5-7, 15-19 Fig. 1** (the ticket being valid for a plurality of trusted computer systems)**]**.

Tait teaches that issuing the ticket (or token, cookie) **[paragraph 0026 lines 9-12]** and the ticket being valid for a plurality of trusted computer system (i.e. resource) **[paragraph 0027 lines 5-7, 15-19 Fig. 1 abstract lines 8-9]**. Tait doesn't expressively mention that *storing said authenticated credential on* said *client* utilizing a security method to prevent tampering with the credential.

Misra teaches that *storing said authenticated credential* **[i.e. logon certificates]** *on* said *client* utilizing a security method to prevent tampering with the credential **[col. 1 lines 57-60 " a secure package that holds certified credential information for the principal. The secure package may be encrypted and/or may include digital signature" lines 62-65 "the secure package may be provide to the principal by storing the secure package in the memory of a portable computer of the user"]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Misra into the teaching of Tait to store authenticated credential on the client. The modification would be obvious because one of ordinary skill in the art would be motivated to connect the distributed system at sites **[Misra, col. 1 lines 19-20]**.

As per claim 4, the rejection of claim 1 is incorporated and Misra teaches:

security method is encryption of the credential (i.e. logon credential) **[col. 4 lines 17-19]**.

As per claim 5, the rejection of claim 1 is incorporated and Misra teaches:

security method is Public Key Infrastructure **[col. 5 lines 22-26]**.

As per claim 6, the rejection of claim 1 is incorporated and it encompasses limitations that are similar to limitations of claim 5. Thus, it is rejected with the same rationale applied against claim 5 above.

4. Claims 2, 3, 7, 8 and 9 are rejected under 35 USC 103 (a) for being unpatentable over Tait (US Pub. No. 2002/0133723) in view of Misra et al (US 5,757,920) in view of Garg et al (US 6,327,677) and in view of McCullough (US 6,865,574).

As per claim 2, the rejection of claim 1 is incorporated and Tait teaches user authentication (i.e. checking the user credential) and using the stored authenticated credential (i.e. ticket) to access said at least one secure resource **[paragraph 0027 lines 5-7, 15-19 Fig. 1** (the ticket being valid for a plurality of trusted computer systems) **abstract, lines 6-9]**.

In addition, Misra teaches that using the stored authenticated credential (i.e. ticket) to access said at least one secure resource **[col. 2 lines 21-23 "the secure package is**

provided to the user (which is stored in the memory) to enable the user to logon to the distributed system"].

Misra teaches that logon certificates are provided to support disconnected operation within the distributed system [abstract lines 1-2]. Tait and Misra don't expressively mention that determining whether the authentication server is in operative or inoperative communication with said client (i.e. monitoring the network connection or communication link between the server and client/device).

However, Garg teaches that determining whether the authentication server is in operative or inoperative communication with said client (i.e. monitoring the network connection or communication link between the server and client/device) **[col. 4 lines 44-53, col. 5 lines 5-8 "monitoring any communication link or interface within a network or between a network and a network device"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Garg into the teaching of Tait and Misra to monitor the network environment. The modification would be obvious because one of ordinary skill in the art would be motivated to detect problems or potential problems in a network environment **[Garg, col. 1 lines 8-9].**

Tait and Misra teach that ticket or logon certificate is expired after predetermine period of time **[Tait paragraph 0028 lines 1-2, Misra col. 4 lines 15-17].** Tait, Misra and Garg don't expressively mention that erasing from said client any stored authenticated credential, if the authentication server is in operative communication with the client (i.e. client is connected to network/server).

McCullough teaches that erasing from said client any stored authenticated credential (i.e. cookie), in response to a determination that the authentication server is in operative communication with the client (i.e. if client is connected to network/server) **[col. 4 lines 30-37 Fig. 3 "user preparing the client computer 12 or a browser running on client computer 12 for use in accessing information at a network site (i.e. client is connected to network/server)" "removing at least the cookies(s) that were placed upon the client computer"].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of McCullough into the teaching of Tait, Misra and Garg to remove the cookies from the client device. The modification would be obvious because one of ordinary skill in the art would be motivated to protect the confidential information regarding to access the remote server **[McCullough, col. 1 lines 58-64].**

As per claim 3, the rejection of claim 2 is incorporated and Tait teaches:

implementing a set of security policies limiting the use of authenticated credentials stored on said client to access said at least one secure resource depending on a defined sensitivity of said at least one resource **[paragraph 0028 lines 1-2].**

In addition, Misra teaches that implementing a set of security policies limiting the use of authenticated credentials stored on said client to access said at least one secure resource depending on a defined sensitivity of said at least one resource **[Fig. 2B, col. 9 lines 34-36, col. 4 lines 15-17].**

As per claim 7, the rejection of claim 2 is incorporated and Misra teaches:

security method is encryption of the credential (i.e. logon credential) **[col. 4 lines 17-**

19].

As per claim 8, the rejection of claim 2 is incorporated and Misra teaches:

security method is Public Key Infrastructure **[col. 5 lines 22-26]**.

As per claim 9, the rejection of claim 2 is incorporated and it encompasses limitations

that are similar to limitations of claim 8. Thus, it is rejected with the same rationale

applied against claim 8 above.

5.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tait (US

Pub. No. 2002/0133723) and in view of Misra et al (US Paten No. 6,189,146).

As per claim 10, Tait teaches:

submitting a user authentication request to said authentication server **[paragraph 0021**

lines 6-10, paragraph 0022 lines 1-3 Fig. 1 (receiving a message form the client at an

authorization module)**]**;

in response to a successful user authentication **[paragraph 0024 lines 1-3 Fig. 1**

(checking the credentials of the client and if valid)**]**;

receiving an authenticated user credential (i.e. ticket) which is unique to said user

[paragraph 0026 lines 10-16 Fig. 1(issuing a ticket to the client)**]**;

using said authenticated credential (i.e. ticket) to access said at least one secure resource **[paragraph 0027 lines 5-7, 15-19 Fig. 1** (the ticket being valid for a plurality of trusted computer systems)**]**.

Tait teaches that issuing the ticket (or token, cookie) **[paragraph 0026 lines 9-12]** and the ticket being valid for a plurality of trusted computer system (i.e. resource) **[paragraph 0027 lines 5-7, 15-19 Fig. 1** (the ticket being valid for a plurality of trusted computer systems) **abstract lines 8-9]**. Tait doesn't expressively mention that *storing said authenticated credential* (i.e. license) *on* said *client* utilizing a security method to prevent tampering with the credential and *storing said authenticated credential* (i.e. license) *on* said *gateway (i.e. intermediate server)* utilizing a security method to prevent tampering with the credential.

However, Misra ('146) teaches that *storing said authenticated credential* (i.e. license) *on* said *client* utilizing a security method to prevent tampering with the credential **[Fig. 3 col. 3 lines 23-25 'the license is passed to the client, where it is stored in a local cache at the client" abstract lines 13-15]** and *storing said authenticated credential* (i.e. license) *on* said *gateway (i.e. intermediate server)* utilizing a security method to prevent tampering with the credential **[Fig. 3, component 32 col. 11 lines 43-45 "the intermediate server 32 also has a legacy license store 130, which stores licenses for clients", lines 53-59]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Misra ('146) into the teaching of Tait to store authenticated credential on client device and on the intermediate server.

The modification would be obvious because one of ordinary skill in the art would be motivated to provide the license/resource to the client when the client doesn't have network connection to the license server (i.e. authentication server is not in operative communication with the client) **[Misra, col. 1 lines 19-20].**

6. Claims 13, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tait (US Pub. No. 2002/0133723) in view of Misra ('146) et al (US Paten No. 6,189,146) and in view of Misra ('920) et al (US 5,757,920).

As per claim 13, the rejection of claim 10 is incorporated and Misra ('920) teaches: security method is encryption of the credential (i.e. logon credential) **[col. 4 lines 17-19].**

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Misra ('920) into the teaching of Tait and Misra ('146) to encrypt the credential (i.e. logon credential). The modification would be obvious because one of ordinary skill in the art would be motivated to provide security to the credential (i.e. logon credential) **[Misra ('920), col. 4 lines 18-19].**

As per claim 14, the rejection of claim 10 is incorporated and Misra ('920) teaches: security method is Public Key Infrastructure **[col. 5 lines 22-26].**

As per claim 15, the rejection of claim 10 is incorporated and it encompasses limitations that are similar to limitations of claim 14. Thus, it is rejected with the same rationale applied against claim 14 above.

7. Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tait (US Pub. No. 2002/0133723) and in view of Misra et al (US Paten No. 6,189,146) in view of Garg et al (US 6,327,677) and in view of McCullough (US 6,865,574).

As per claim 11, the rejection of claim 10 is incorporated and Tait teaches user authentication (i.e. checking the user credential) and using the stored authenticated credential (i.e. ticket) to access said at least one secure resource **[paragraph 0027 lines 5-7, 15-19 Fig. 1 abstract, lines 6-9].**

In addition, Misra ('146) teaches that using the stored authenticated credential (i.e. license) to access said at least one secure resource **[Fig. 3 component 30]** and stored authenticated credential (i.e. license) on the gateway (i.e. intermediate server) **[Fig. 3 component 32].** Misra ('146) teaches that gateway (i.e. intermediate server) provides the license/resource to the client when the client doesn't have the network connection to the license server (i.e. authentication server is not in operative communication with the client) **[col. 1 lines 19-20].**

Tait and Misra don't expressively mention that determining whether the authentication server/gateway is in operative or inoperative communication with said client (i.e.

monitoring the network connection or communication link between the server and client/device).

However, Garg teaches that determining whether the authentication server/gateway (i.e. network device) is in operative or inoperative communication with said client (i.e. monitoring the network connection or communication link between the server and client/device) **[col. 4 lines 44-53, col. 5 lines 5-8 "monitoring any communication link or interface within a network or between a network and a network device (gateway, router, server etc)"]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Garg into the teaching of Tait and Misra to monitor the network environment. The modification would be obvious because one of ordinary skill in the art would be motivated to detect problems or potential problems in a network environment **[Garg, col. 1 lines 8-9]**.

Tait and Misra teach that ticket or logon certificate is expired after predetermine period of time **[Tait paragraph 0028 lines 1-2, Misra col. 4 lines 15-17]**. Tait, Misra and Garg don't expressively mention that erasing from said client any stored authenticated credential, if the authentication server is in operative communication with the client (i.e. client is connected to network/server).

McCullough teaches that erasing from said client any stored authenticated credential (i.e. cookie), in response to a determination that the authentication server is in operative communication with the client (i.e. if client is connected to network/server) **[col. 4 lines 30-37 Fig. 3 "user preparing the client computer 12 or a browser running on client**

computer 12 for use in accessing information at a network site (i.e. client is connected to network/server)" "removing at least the cookies(s) that were placed upon the client computer"].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of McCullough into the teaching of Tait, Misra and Garg to remove the cookies from the client device. The modification would be obvious because one of ordinary skill in the art would be motivated to protect the confidential information regarding to access the remote server [McCullough, col. 1 lines 58-64].

As per claim 12, the rejection of claim 11 is incorporated and Tait teaches:

implementing a set of security policies limiting the use of authenticated credentials stored on said client to access said at least one secure resource depending on a defined sensitivity of said at least one resource [paragraph 0028 lines 1-2].

In addition, Misra('146) teaches that implementing a set of security policies limiting the use of authenticated credentials stored on said client to access said at least one secure resource depending on a defined sensitivity of said at least one resource [Table 5, col. 11, expiration date].

8. Claims 16, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Tait (US Pub. No. 2002/0133723) and in view of Misra et al (US Paten No.

6,189,146) in view of Garg et al (US 6,327,677) in view of McCullough (US 6,865,574)

and in view of Misra ('920) et al (US 5,757,920).

As per claim 16, the rejection of claim 11 is incorporated and Misra ('920) teaches:

security method is encryption of the credential (i.e. logon credential) **[col. 4 lines 17-**

19].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time

the invention was made to incorporate the teaching of Misra ('920) into the teaching of

Tait, Misra ('146), Garg and McCullough to encrypt the credential (i.e. logon credential).

The modification would be obvious because one of ordinary skill in the art would be

motivated to provide security to the credential (i.e. logon credential) **[Misra ('920), col.**

4 lines 18-19].

As per claim 17, the rejection of claim 11 is incorporated and Misra ('920) teaches:

security method is Public Key Infrastructure **[col. 5 lines 22-26].**

As per claim 18, the rejection of claim 11 is incorporated and it encompasses limitations

that are similar to limitations of claim 17. Thus, it is rejected with the same rationale

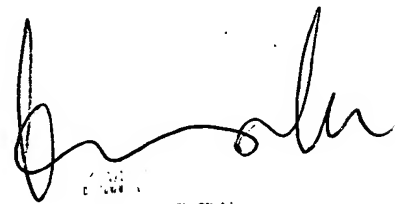applied against claim 17 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NBP
12/29/05